

Vote for a strong sovereign Europe that can guarantee data protection rights to its citizens and control the EU Trust Space – eIDAS Art. 45

ESD asks all Members of the European Parliament to support the Commission's proposal¹ for amendments to eIDAS Article 45 where requirements for QUALIFIED CERTIFICATES FOR WEBSITE AUTHENTICATION (QWACs) are regulated. The wording of the Commission proposal ensures that Consumers are empowered, and that Europe can continue to guarantee a high level of data protection and control its own Trust Space, as described below.

Any attempt to water down the proposed Article 45 is rejected by ESD as this can have dangerous consequences for transparency and consumer protection as well as European sovereignty in data protection legislation and Qualified trust services. Serious concerns have already been raised by antitrust authorities² over the demands by Big Tech browsers to dilute the Commission's proposal.

It is important that paragraph 3 of Article 45 is updated to also require implementing acts that specify requirements, transparent procedures, timelines, and mechanisms to respond to any objections of browsers on the recognition and display of QWACs. These implementing acts could address concerns raised by Big Tech browsers regarding the trustworthiness and supervision of individual Qualified Trust Service Providers. However, the display of identity information about the website owner to Relying Parties (EU citizens) is *non-negotiable*, as it is a fundamental and existing *right* of EU citizens to know who they are interacting with when providing personal data.

The European Signature Dialog (ESD)³ represents the leading European trust service providers (TSPs). TSPs enable secure digital interactions across Europe - between public entities, businesses, and individuals. All ESD members are working ceaselessly to enable trust, transparency, security, and protection of consumers on the internet every day according to **top EU standards**. Big tech browsers have not cooperated with the goals of eIDAS since its enactment in 2014, which the Commission is now addressing.

(1) Accepting and displaying QWACs is essential to protect EU consumers, fight cybercrime and build a strong European Digital Single Market

With the proposed Article 45 for an amended eIDAS Regulation the Commission proposes two new elements:

¹ Brussels 3.6.2021, COM (2021) 281 final

² Bundeskartellamt, the German Anti-trust authority – see point 3 of position paper (page 3)

³ <https://www.european-signature-dialog.eu/>

1. It requires browsers to display in a **user-friendly manner** the **identity** of the **person or organization** operating a QWAC-certified website. This identity display is needed to strengthen transparency and trust, and also to comply with the EU's "**right to know**" and **GDPR**⁴ laws.
2. It strengthens QWACs (which are a European standard), by clarifying that browsers **can no longer unilaterally refuse to trust QWACS** issued by **Qualified Trust Service Providers (QTSPs)** that are on the EU Trusted Lists⁵ and which enable the encryption of data to websites and provide the website operators' identity information to EU citizens. Some client software such as Adobe Acrobat have simply adopted the EU Trusted Lists of QTSPs as defined by Article 22 of the eIDAS regulation – **and browsers should do the same.**

With the proposed Article 45 for an amended eIDAS Regulation the Commission takes an important step to protect and empower citizens using secure digital identities and trust services in the European Union. Here are examples:

- ✓ Consumers **can see the identity of website owners** (e.g., their bank) before providing personal data such as username or account number. *(A study by RWTH Aachen University shows **how important proof of identity** is: The study found that 99.6% of all **phishing attacks** originate from non-identity certificate-secured websites).*⁶
- ✓ Law enforcement can track the actions of websites and their owners, **giving them recourse** when websites engage in fraud or phishing.
- ✓ This is important for more transparency, consumer protection and enforcement of EU laws on the "right to know". In this way, the **EU will control decisions on its digital sovereignty, not non-EU Big Tech companies.**

(2) Watering down/Rejecting the Commission proposal means that Big Tech companies/browsers will establish exclusive control over security rules and user interfaces, thus stripping the EU of its legislative power to provide a secure, safe and transparent Internet for its citizens

Browsers and the Electronic Frontier Foundation (EFF), who are heavily intertwined and share common interests in not providing any identity information to the user⁷, have rejected the

⁴ General Data Protection Regulation. See also the law on Consumer rights 2011/83/EU, Article 6, which includes a "right to know" regarding the identity of websites and the law on Services in the internal market 2006/123/EC, Article 22.

⁵ Member States have the obligation to establish trusted lists of QTSPs and the services provided by them. National trusted lists have a constitutive effect: a trust service provider and the trust services it provides will be qualified only if it appears in a trusted list.

⁶ <https://www.usenix.org/system/files/soups2019-drury.pdf> (See pages 8-9)

⁷ The largest certification authority in the world is a US-based company called "Let's Encrypt". It was established in 2014 and *currently has a staggering 56.6% of the entire certificate market – worldwide*. Let's Encrypt certificates do not provide any identity information to the user.

Let's Encrypt's receives "Platinum Level" funding from EFF and non-EU Big Tech companies such as Google, Mozilla, Facebook, Amazon, and Cisco.⁷ Representatives of EFF and some of the browsers serve on the Board and Technical Advisory Board of Let's Encrypt's parent organization ISRG. In other words, the browsers and EFF are totally entwined with Let's Encrypt and responsible for its policies.

Commission proposal based on flimsy and unsubstantiated concerns. None of their arguments is supported by factual evidence or detailed reasoning.

Their demands actually contradict existing EU law on a user's "right to know" who they are dealing with, especially as to personal data (passwords, credit card numbers) that anonymous websites may request and use for fraud or phishing.

While the browser/ EFF statements in opposition to the Commission proposal do not use these exact words, ***here is what rejecting Art. 45 (2) would mean:***

- ✓ Recognizing QWACs and displaying identity data to users serves to recognize existing and established European standards. **By rejecting these established European standards, web-browsers (mostly non-EU Big Tech companies) would have exclusive control over the security rules for the internet.** The European Union would have no role at all in setting the standards for the EU digital sovereignty and the security of EU citizens.
- ✓ Big Tech web browsers would also have **exclusive control over the user interfaces that display website identity information to EU citizens.** If the browsers decide to hide QWAC website identity information from EU citizens (as they do today) or confuse users with different implementations between browsers (as they did historically), they would be entitled to do so.

As a consequence, the **EU would have no power at all to set requirements** for websites that ask for personal – or even sensitive - data of EU citizens. Under current EU law, websites should first *identify* themselves to the user *before* asking for personal data. Browsers, EFF, and their supporters are opposed to this identity disclosure to consumers - although they never say why.

These browser/EFF arguments against Article 45 are not correct, and it's dangerous for all power over internet security to be in the hands of private non-EU "gatekeepers" driven by commercial interests.

The European Commission's DG Connect has already stated that it strongly disagrees with these browser/ EFF arguments.

(3) Germany's antitrust authority has serious concerns that past browser actions and opposition to eIDAS Article 45 may violate both EU and German antitrust law

In this context it's worth noting that Google has **recently been investigated by** the German Bundeskartellamt antitrust agency for possible violations *in exactly these two areas* which will be covered by the eIDAS Article 45 amendments.

The Bundeskartellamt stated that **a user-friendly display of QWAC certificate identity information by the browsers** as well as general rules preventing the withdrawal of trust of QTSPs by browsers "**could only be achieved with legal requirements** - e.g., in the course of the revision of the eIDAS Regulation at European level" that is currently before the Parliament.

The Bundeskartellamt noted that the proposed eIDAS Article 45 legislation would **solve the “user friendly” User Interface issue**, and on this basis, it decided to terminate its investigation⁸. If eIDAS Article 45 is now blocked in Parliament, it’s possible the Bundeskartellamt could reopen its investigation, but as stated in the report it’s unlikely that a decision by the Bundeskartellamt in Germany against one browser alone will result in the maximum conceivable added value of more trustworthy certificates across Europe.

ESD therefore pleads with all MEPs to support the Commission’s legislative solution for Article 45 that is compatible with national and European competition rules and law.

Summary of important points:

ESD asks MEPs to **support** eIDAS Article 45 because

- ✓ Accepting and displaying QWAC identity information to users is **essential to protect consumers, fight cybercrime** and build a **strong European Digital Single Market**
- ✓ **Watering down/rejecting the Commission proposal** means that **Big Tech companies/browsers will establish exclusive control** over security rules and user interfaces in Europe, thus **stripping the EU of its legislative power** to provide a secure, safe and transparent Internet and controlling the EU trust space
- ✓ Germany’s **antitrust authority has serious concerns** that past browser actions and opposition to Article 45 eIDAS review may **violate both EU and German antitrust law**
- ✓ The European Commission’s DG Connect has stated that it strongly disagrees with the arguments against Article 45 presented by browser/ EFF. These arguments are vague and not supported

We urge all MEPs to support the Commission’s eIDAS Article 45 provisions.

In case you wish more information please write or call us:

European Signature Dialog

EU Transparency Register number: 994150833943-81

Mail to office@european-signature-dialog.eu

This position is supported by the following organizations:



**PKI
Consortium**

The PKI Consortium is comprised of leading organizations that are committed to improve, create and collaborate on generic, industry or use-case specific policies, procedures, best practices, standards and tools that advance trust in assets and communication for everyone and everything using Public Key Infrastructure (PKI) as well as the security of the internet in general. <https://pkic.org>

⁸ https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2022/B7-250-19.pdf?__blob=publicationFile&v=4 See pages 2-4, 6-7 and 9.



Eurosmart, the Voice of the Digital Security Industry, is a European non-profit association located in Brussels, representing the Digital Security Industry for multisector applications. Founded in 1995, the association is committed to expanding the world's digital secure devices market, developing smart security standards and continuously improving the quality of security applications.

<https://www.eurosmart.com/>